Gavin Pearce MP
Federal Member for Braddon

Media Release

22 November 2023

Underwhelming cyber strategy too little too late

The Albanese government's new cyber security strategy, to be finally released today after more than a year in development and millions spent on high-priced consultants, fails to live up to the expectations minister O'Neil set for the government.

With only $587 million of investment, it pales in comparison to the $1.67 billion from the 2020 Cyber Security Strategy and the $9.9 billion injection into the Australian Signals Directorate under the REDSPICE program under the former government.

After announcing in August 2022 that she was going to "tear up" the existing cyber security strategy to make Australia the most cyber secure country in the world by 2030, Home Affairs and Cyber Security Minister Clare O'Neil has now unveiled a series of minor tweaks and logical extensions of the previous government's policies.

There is nothing radical or revolutionary in the Strategy, nor anything that will substantially shift the dial on cyber security. Rhetoric does not equate to action, and it is striking just how far the Strategy falls short of the Minister's self-stated ambition to make Australia the most cyber secure nation in the world by 2030.

The Strategy has been launched after 15 months of development, and more than a year after the Optus and Medibank cyber incidents that rocked Australia last year. Australians expected government to act sooner, and today has revealed the final Strategy was not worth the wait.

Many of the key elements of the Strategy could and should have been implemented months ago and have been called for by stakeholders and the Opposition for some time.

For example, the proposal for a "safe harbour" or confidential sharing mechanism for companies subject to a cyberattack was first called for by the Opposition on 22 March 2023 and has been repeatedly publicly endorsed by ASD Director General Rachel Noble. Despite the announcement in the strategy, we still don't have any clarity on when this straightforward but important change will actually be legislated.

Likewise, the Opposition first called on the government to establish a post incident review board in October, and if the government had moved more quickly this construct could have been up and running to assist with recent cyber incidents like the one impacting DP World earlier this month.

Based on media reports so far, there remain number of glaring omissions from the Strategy. After the Opposition identified almost 1,000 high-risk CCTV cameras, more than 3,000 unsafe drones, and widespread usage of risky apps like TikTok and WeChat within the federal government, the Strategy fails to provide a comprehensive plan to deal with high-risk authoritarian vendors.

And despite Minister O'Neil announcing she had commissioned a review from her department on the risks of foreign interference through social media in our democracy, the Strategy appears silent on this serious threat.

Despite the fanfare, today's much delayed cyber strategy has ultimately oversold and under delivered. It is a major flop that falls well-short of ensuring Australia will become the most cyber-secure country in the world by 2030, and Australians deserve better.

ENDS